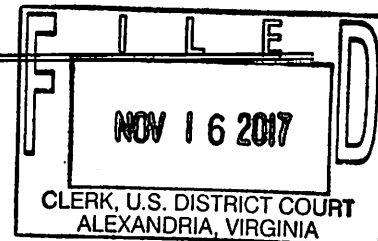


UNDER SEAL
UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

INFORMATION ASSOCIATED WITH
borntowin88@icloud.com THAT IS STORED AT
PREMISES CONTROLLED BY APPLE, INC.

Case No. 1:17sw 780

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 924(c)

21 U.S.C. §§ 841(a)(1), 846

Offense Description

Use and Carry of a Firearm During and in Relation to a Drug Trafficking Crime
Conspiracy to Distribute and Possess with the Intent to Distribute Controlled
Substances

The application is based on these facts:
See attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Colleen E. Garcia

Jonathan Boller

Applicant's signature
Jonathan C. Boller, ATF Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 16 Nov 17

City and state: Alexandria, VA

ICD /s/ _____
Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with borntowin88@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, California 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs,

iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

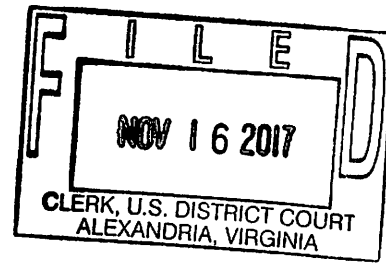
All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of conspiracy to distribute and possession with intent to distribute cocaine and other controlled substances, in violation of Title 21, United States Code, Sections 841(a)(1) and 846, and the use and carry of a firearm during and in relation to a drug trafficking crime, involving TARVELL VANDIVER since October 6, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Any photographs of firearms, ammunition, firearms receipts, and documentation related to the purchase of firearms;
- b. Any photographs of cocaine, marijuana, THC, or other controlled substances, and drug paraphernalia;
- c. Any photographs of currency or other possible proceeds of the sale of controlled substances or firearms;
- d. Any photographs of means of transportation or housing;
- e. Any notes related the purchase or sell of controlled substances and firearms;
- f. iMessages and messages on other Applications between VANDIVER and other co-conspirators concerning the sale of controlled substances and firearms;
- g. Calendar entries for meetings of the Imperial Gangster Blood gang;
- h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

k. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

l. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts. These co-conspirators include, but are not limited to, Ishmil Hardwick, Rashourn Niles, Nasiru Carew, Jerry McAllister, Anthony Lozada, Tyrus Terrel, Sade Anglin, Nathaniel Bruce Cobbold, Kevin Crews, and Montreus Peterson.



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
borntowin88@icloud.com THAT IS
STORED AT PREMISES CONTROLLED
BY APPLE, INC.

Under Seal

Case No. 1:17sw780

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jonathan C. Boller, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with Apple ID borntowin88@icloud.com (hereinafter the "SUBJECT ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B. This is the third request for a search warrant. On April 3, 2017, the Honorable John F. Anderson, Magistrate Judge for the Eastern District of Virginia authorized a search warrant for the subject account. On October 6, 2017, the Honorable Theresa Carroll Buchanan, Magistrate Judge for the Eastern District of Virginia authorized a second search warrant for the subject account from April 3, 2017 to October 6, 2017. This third search warrant is to obtain the information in Attachment B from October 6, 2017 to the present.

2. I have been a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") since 2016. I have experience investigating narcotics and firearms trafficking offenses.

3. As an ATF Special Agent, I have investigated and assisted in the investigation of narcotics and firearms traffickers. I have previously participated in investigations, which resulted in the arrest and conviction of narcotics and firearms traffickers. I have also become familiar with the methods and techniques associated with the distribution of narcotics and how drug trafficking organizations work. From 2014 to 2016, I served as a Special Agent with the United States Secret Service, where I received specialized training including certification in the Basic Investigation of Computer and Electronic Crimes Program.

4. Further, through instruction, training, and participation in investigations, as well as through consultation with other agents and law enforcement personnel, I have become familiar with the manner in which narcotics traffickers conduct their illegal business and the methods used to disguise their narcotics activities. From experience and training, I have also learned that narcotics traffickers frequently use encrypted cellular telephone applications, cellular phone services, and other technologies to communicate, conduct, and conceal their illegal activities from law enforcement.

5. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations of Title 18, United States Code, Section 924(c) (use and carry of a firearm during and in relation to a drug trafficking offense) and Title 21, United States Code, Sections 841(a)(1) and 846 (conspiracy to distribute and possess with the intent to distribute Cocaine and other controlled substances), as described in Attachment B.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

A. Background on the Investigation

7. In February 2017, a cooperating source ("CI-1") reported to the Prince William County Police Department that TARVELL VANDIVER was a narcotics distributor. CI-1 is a member of the Imperial Gangster Blood gang. CI-1 will be referred to in the masculine gender, regardless of CI-1's true gender. CI-1 has been convicted of two felonies, including robbery and a probation violation. He was arrested in December of 2016, in Prince George's County, Maryland, for possessing a stolen firearm as a convicted felon and possession of controlled substances. CI-1 originally cooperated because he hoped to receive a lesser sentence. Based on CI-1's cooperation, Prince George's County dismissed his charges. CI-1 continues to cooperate because he is being compensated. CI-1 also hopes to be relocated.

8. Based on this information and because VANDIVER is a known member of the Imperial Gangster Blood gang, ATF opened an investigation into VANDIVER.

B. First Search Warrant for the SUBJECT ACCOUNT on April 3, 2017

9. As stated above, on April 3, 2017, the Honorable John F. Anderson authorized a search warrant for the SUBJECT ACCOUNT. I have reviewed the returns for the SUBJECT ACCOUNT. The return from Apple includes critical information that corroborates that VANDIVER is a member of a conspiracy to distribute controlled substances.

10. The information supplied by Apple in response to the search warrant included information that documented communication between parties using FaceTime. This information is not included in the information supplied by a court authorized pen register and trap and trace device. This information specifically provided the phone numbers that VANDIVER communicated with on dates and times when other evidence supports that VANDIVER was arranging the sale of or was personally selling cocaine and other illegal substances or firearms. The phone numbers for multiple suspected co-conspirators were also included in records supplied by Apple. Further, CI-1 states that VANDIVER uses FaceTime to conceal records of his communications. Thus, VANDIVER uses FaceTime as his primary means to communicate with co-conspirators, when he is arranging the distribution of cocaine and other controlled substances.

11. Since April 3, 2017, as explained below, VANDIVER has continued to use FaceTime to communicate with co-conspirators and arrange drug transactions. There is probable cause to believe that communication records for the SUBJECT ACCOUNT will once again corroborate when and with whom VANDIVER was communicating.

C. Controlled Purchase of Cocaine from Tarvell Vandiver on March 30, 2017

12. On March 30, 2017, CI-1 contacted VANDIVER on FaceTime and VANDIVER advised that he was at the Potomac Mills Mall. VANDIVER's FaceTime account is linked to the SUBJECT ACCOUNT. At law enforcement direction, CI-1 drove to the mall and met with VANDIVER. Both CI-1 and VANDIVER then entered VANDIVER's vehicle and made contact via phone with a co-conspirator ("Co-Conspirator 1"). Co-Conspirator 1 advised that he had just obtained seven (7) grams of heroin and CI-1 was welcome to travel to his residence and purchase heroin. After the call, VANDIVER drove CI-1 to 14309 Bellona Road, Woodbridge, Virginia.

VANDIVER and CI-1 then entered an apartment, where VANDIVER weighed out approximately 130 grams of cocaine and provided it to CI-1 in exchange for \$5,400.

13. VANDIVER then drove with CI-1 in VANDIVER's vehicle to the Coastal Station located at 2010 Old Bridge Road, Woodbridge, Virginia. VANDIVER then sold a half ounce of cocaine to an unidentified male. VANDIVER's movements were observed by law enforcement and later confirmed by CI-1.

14. VANDIVER then returned with CI-1 to Potomac Mills Mall, where CI-1 secured the cocaine that he purchased from VANDIVER in the glove box of his vehicle. CI-1 then returned to VANDIVER's vehicle. Law enforcement maintained surveillance on CI-1's vehicle in the parking lot until the operation was concluded.

15. VANDIVER then contacted Co-Conspirator 1 and arranged to meet at Co-Conspirator 1's residence in order for CI-1 to purchase heroin. VANDIVER later drove CI-1 to Co-Conspirator 1's residence and VANDIVER again contacted Co-Conspirator 1 to let him know that they had arrived. Co-Conspirator 1 came out of his residence and entered VANDIVER's vehicle. While in the vehicle, Co-Conspirator 1 sold four (4) grams of heroin to CI-1 for \$300.

16. VANDIVER then drove CI-1 back to CI-1's vehicle located at the Potomac Mills Mall. CI-1 drove to a meeting location where law enforcement debriefed CI-1. CI-1 provided law enforcement with the suspected cocaine, which field-tested positive for the presence of cocaine. CI-1 also provided law enforcement with the suspected heroin, which field-tested positive for the presence of heroin.

D. Controlled Purchase of Crack Cocaine from Tarvell Vandiver on April 6, 2017

17. At the direction of law enforcement, CI-1 contacted VANDIVER and arranged to purchase two (2) ounces of crack cocaine and one (1) ounce of cocaine from VANDIVER. VANDIVER also advised that he would manufacture the cocaine into crack cocaine. While CI-1 was on his way to meet VANDIVER, VANDIVER called CI-1 on FaceTime and asked CI-1 to pick up some baking soda (which is a common ingredient used to make crack cocaine). CI-1 then travelled to the area where he and VANDIVER had arranged to meet. VANDIVER then advised CI-1 on FaceTime to come to the apartment on Bellona Road.

18. CI-1 met VANDIVER outside of the apartment and the two entered the apartment together. According to CI-1, VANDIVER then took a phone call from a subject who placed an order for cocaine. While in the apartment, CI-1 stated that VANDIVER instructed him in the crack cocaine manufacturing process, including how much baking soda to mix with the cocaine. CI-1 observed VANDIVER manufacturing powder cocaine into crack cocaine by using baking soda, water, and a microwave to heat the mixture.

19. VANDIVER then received an incoming phone call and agreed to meet a co-conspirator at the McDonald's located on Dale Boulevard. VANDIVER and CI-1 then left the apartment, and while being surveilled by law enforcement, travelled to a McDonald's Restaurant located at 2891 Dale Blvd, Dale City, Virginia. VANDIVER was then observed exiting his vehicle and meeting with a co-conspirator. CI-1 later confirmed that VANDIVER sold an unknown amount of cocaine to the co-conspirator.

20. VANDIVER then drove CI-1 to various other locations and then returned to the apartment located at 14309 Bellona Road. VANDIVER then placed an outgoing FaceTime call to another co-conspirator ("Co-Conspirator 2") and explained that the crack cocaine was still

soft. Co-Conspirator 2 then advised VANDIVER how to complete the drying process. CI-1 observed this FaceTime call and observed VANDIVER using a microwave and hairdryer to complete the hardening process of the crack cocaine. VANDIVER then made further statements advising CI-1 how to maximize his crack cocaine yield during the manufacturing process.

21. CI-1 then provided \$4,900 to VANDIVER in exchange for two (2) ounces of crack cocaine and one (1) ounce of cocaine. CI-1 then drove to a meeting location where law enforcement debriefed CI-1. CI-1 provided law enforcement with the suspected cocaine, which field-tested positive for the presence of cocaine. While law enforcement ordered and paid for two ounces of crack cocaine, the purchased quantity weighed approximately 112 grams.

E. Controlled Purchase of Cocaine and a Firearm from Tarvell Vandiver on May 9, 2017

21. In the days leading up to May 9, 2017, VANDIVER contacted CI-1 and asked if he (CI-1) wanted to purchase a firearm. At law enforcement direction, CI-1 agreed to purchase a firearm and ordered one (1) ounce of cocaine. CI-1 estimated the firearm and cocaine would cost approximately \$2,000.

22. Prior to the controlled purchase, law enforcement searched CI-1 and his vehicle and found it to be free of any illegal contraband. Law enforcement then provided CI-1 with ATF agent cashier funds to conduct the controlled purchase. The controlled purchase was also audio recorded.

23. After departing the staging location, CI-1 contacted VANDIVER via FaceTime =, which is linked to the SUBJECT ACCOUNT, and was instructed to meet VANDIVER at a location on Bayside Avenue, Woodbridge, Virginia. Upon meeting VANDIVER in the parking lot, CI-1 entered his vehicle. VANDIVER and CI-1 were observed driving to a gas station and then returning to the apartment on Bayside Avenue. Inside the apartment, CI-1 was sitting when

VANDIVER asked him if he felt anything. When CI-1 shifted his weight, he could feel something inside a pillow. CI-1 opened the zipper and later reported VANDIVER cutout a portion of the foam inside one of the cushions. CI-1 located approximately 4.5 ounces of powder cocaine inside clear plastic baggies. VANDIVER stated that if law enforcement ever found the drugs hidden inside the pillow, that law enforcement could not prove his knowledge of the cocaine because he does not reside in the apartment.

24. VANDIVER told CI-1 the price of cocaine increased from \$1,300 to \$1,400 and CI-1 agreed. VANDIVER placed the 4.5 ounces of cocaine on the dining room table, weighed out one (1) ounce and placed it in a plastic bag. VANDIVER also told CI-1 he was trying to make a \$300 profit from the firearm CI-1 was going to purchase. CI-1 agreed and provided VANDIVER with \$2,000 in ATF agent cashier funds for the firearm and cocaine. CI-1 took custody of the cocaine that he purchased and VANDIVER took custody of the remainder of the cocaine.

25. VANDIVER and CI-1 then exited the apartment and entered VANDIVER's vehicle. Law enforcement followed CI-1 and VANDIVER to a location within the Eastern District of Virginia, where VANDIVER was observed entering an apartment. VANDIVER returned to his vehicle with a towel in his hand and was seen wiping an unidentified object. Upon entering the vehicle, VANDIVER placed the firearm wrapped in a towel on the driver's seat near his legs.

26. CI-1 and VANDIVER then drove in the VANDIVER's vehicle back to the Bayview Apartment complex and CI-1 entered his vehicle. Upon arriving at the complex, VANDIVER handed CI-1 the firearm, which was a Smith & Wesson .40 caliber pistol, wrapped in the towel. VANDIVER then left.

27. CI-1 was followed to a meeting location where law enforcement debriefed CI-1. CI-1 provided law enforcement with the suspected cocaine and firearm. The cocaine field-tested positive for the presence of cocaine and had a field weight of approximately 30 grams.

F. Purchase of two firearms from a Co-Conspirator in a deal setup by Tarvell Vandiver

28. On July 27, 2017, CI-1, at law enforcement direction, contacted VANDIVER with the goal of obtaining firearms and distribution quantities of marijuana. The communication occurred through FaceTime with CI-1 contacting VANDIVER on the SUBJECT ACCOUNT. During this communication, and throughout the entirety of their association, CI-1 states that VANDIVER would have been aware that CI-1 is a convicted felon. Later that same day VANDIVER sent CI-1 images of the firearms that were available for sale. Then, a co-conspirator sent his address to VANDIVER via Snapchat. CI-1 later purchased two firearms from VANDIVER for \$1,300.

29. On August 16, 2017, United States Magistrate Judge John F. Anderson, authorized a search warrant for the contents of the Snapchat account for the co-conspirator that contacted VANDIVER via Snapchat. The communication log of this account shows multiple communications and images of the same firearms purchased by CI-1 from VANDIVER on July 27, 2017.

G. Controlled Purchases of Controlled Substances from Tarvell Vandiver since April 26, 2017

30. At law enforcement direction, CI-1 has continued to purchase controlled substances, including powder cocaine, crack cocaine, heroin, and marijuana from VANDIVER. During this entire time period, CI-1 has communicated with VANDIVER via FaceTime and iMessage. VANDIVER uses the SUBJECT ACCOUNT for his FaceTime calls and iMessages.

H. Second Search Warrant Issued for SUBJECT ACCOUNT on October 6, 2017

31. On October 6, 2017, United States Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia issued a search warrant for the SUBJECT ACCOUNT. The response to the search warrant from Apple, along with subsequent conversations with Apple's technical staff, has revealed that Apple only stores Facetime connections logs for approximately 2 to 3 weeks.

I. Tarvell VANDIVER facilitation of ½ kilo Cocaine purchase October 30, 2017

32. On October 30, 2017, CI-1, at law enforcement direction, was socializing with Tarvell VANDIVER. While physically present with VANDIVER inside his apartment, CI-1 placed an order through VANDIVER for a ½ kilo, or approximately 18 ounces, of Cocaine. CI-1 stated to law enforcement that after he placed the order through VANDIVER, VANDIVER contacted Co-Conspirator 2 through a series of Facetime and voice (telephone) calls. CI-1 further stated that VANDIVER then told CI-1 that Co-Conspirator 2 would contact individuals he (Co-Conspirator 2) believed would be able to handle a transaction of that size. Approximately 45 minutes later, an individual arrived in the parking lot of VANDIVER's apartment building. VANDIVER exited his apartment and made contact with the individual in the car. VANDIVER exchanged \$19,950 in ATF buy money for what later field tested positive as Cocaine, and field measured to be approximately 515 grams.

31. A preservation request for the SUBJECT ACCOUNT was sent to Apple on October 20, 2017 with receipt confirmed by Apple the same day.

32. As detailed above, VANDIVER is using iMessage and FaceTime to facilitate the distribution of cocaine and other controlled substances and to arrange firearms transactions.

Based on these facts and the other facts detailed in this affidavit, I submit there is probable cause to suspect that VANDIVER used and continues to use his Apple iPhone to sell controlled substances and arrange firearms transactions. I therefore submit there is probable cause to believe that iMessages, photographs, and other evidence as detailed in Attachment B could be stored in VANDIVER's iCloud account.

INFORMATION REGARDING APPLE ID AND iCloud¹

33. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

34. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "iCloud: iCloud storage and backup overview," available at <https://support.apple.com/kb/PH12519>; and "iOS Security," available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or

Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

35. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

36. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

37. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

38. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

39. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

40. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

41. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of Cocaine sales and firearm sales, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

42. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often

created and used in furtherance of narcotics and firearms trafficking, including to communicate and facilitate the sale of narcotics and firearms.

43. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

44. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. For instance, based on my experience investigating narcotics and firearms traffickers, I know that traffickers frequently communicate

using the following applications, but not limited to, WhatsApp, Instagram, Telegram, Facebook Messenger etc. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

46. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

47. Based on the above examples, I therefore submit that information stored on Apples servers will show evidence of the crimes of conspiracy to distribute controlled substances and the use and carry of a firearm during and in relation to a drug trafficking crime. More specifically, and as previously stated, there is probable cause to support that the user information, IP addresses, photographs, text messages, and apps downloaded will show evidence that VANDIVER distributes controlled substances and/or possesses firearms while distributing controlled substances.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

48. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

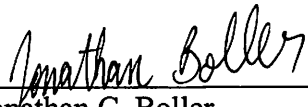
49. Based on the forgoing, I request that the Court issue the proposed search warrant.

50. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that — has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

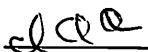
REQUEST FOR SEALING

52. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.



Jonathan C. Boller
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Sworn and subscribed to before me this 16th day of November.

 /s/ _____
Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with borntowin88@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, California 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs,

iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of conspiracy to distribute and possession with intent to distribute cocaine and other controlled substances, in violation of Title 21, United States Code, Sections 841(a)(1) and 846, and the use and carry of a firearm during and in relation to a drug trafficking crime, involving TARVELL VANDIVER since October 6, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Any photographs of firearms, ammunition, firearms receipts, and documentation related to the purchase of firearms;
- b. Any photographs of cocaine, marijuana, THC, or other controlled substances, and drug paraphernalia;
- c. Any photographs of currency or other possible proceeds of the sale of controlled substances or firearms;
- d. Any photographs of means of transportation or housing;
- e. Any notes related the purchase or sell of controlled substances and firearms;
- f. iMessages and messages on other Applications between VANDIVER and other co-conspirators concerning the sale of controlled substances and firearms;
- g. Calendar entries for meetings of the Imperial Gangster Blood gang;
- h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- i. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

j. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

k. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

l. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts. These co-conspirators include, but are not limited to, Ishmil Hardwick, Rashourn Niles, Nasiru Carew, Jerry McAllister, Anthony Lozada, Tyrus Terrel, Sade Anglin, Nathaniel Bruce Cobbold, Kevin Crews, and Montreus Peterson.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____. I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and
- c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature